

## UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of an Apple iPhone 12 Taken )  
 Off of the Person of Bryce Pyle Incident to His Arrest, )  
 Currently Stored at a Secured Facility Controlled by the )  
 Tulsa Police Department )

Case No.

24-mj-515-JFJ

**FILED**  
 JUL 31 2024  
 Heidi D. Campbell, Clerk  
 U.S. DISTRICT COURT

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 1151, 1153, 21 O.S. §§ 1431 and 1436 First Degree Burglary

18 U.S.C. §§ 1151, 1153 and 113(a)(3) Assault with Intent to do Bodily Harm in Indian Country

18 U.S.C. § 924(c)(1)(A)(iii) Discharging a Firearm During and in Relation to a Crim of Violence

The application is based on these facts:

See Affidavit of FBI Special Agent Audra Rees, attached hereto.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

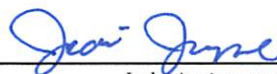
FBI Special Agent Audra Rees

Printed name and title

Subscribed and sworn to by phone.

Date: 7/31/24

City and state: Tulsa, Oklahoma



*Judge's signature*

Jodi F. Jayne, U.S. Magistrate Judge

*Printed name and title*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of  
An Apple iPhone 12 Taken Off of the  
Person of Bryce Pyle Incident to His  
Arrest, Currently Stored at a Secured  
Facility Controlled by the Tulsa Police  
Department**

**Case No.**

**Affidavit in Support of an Application  
Under Rule 41 for a Warrant to Search and Seize**

I, Special Agent Audra Rees, being first duly sworn under oath, depose and state as follows:

**Introduction and Agent Background**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C). Therefore, I am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of federal officers authorized by the Attorney General to request such a warrant. I have been employed as a Special Agent with the Federal Bureau of Investigations (“FBI”) since 2020. I am currently assigned to the Tulsa RA of the

Oklahoma City Division. As a result of my employment with the FBI, my duties include, but are not limited to, the investigation and enforcement of domestic violence, sexual assault, kidnapping, witness tampering, gun crimes, and other violent crimes.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and knowledge of the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1151, 1153, 21 O.S. §§ 1431, and 1436 – First Degree Burglary; 18 U.S.C. §§ 1151, 1153, and 113(a)(3) – Assault with Intent to do Bodily Harm in Indian Country; and 18 U.S.C. § 924(c)(1)(A)(iii) – Discharging a Firearm During and in Relation to a Crime of Violence will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

### **Identification of the Device to be Examined**

5. The property to be searched is an Apple iPhone 12 taken off of the person of Bryce Pyle incident to his arrest, hereinafter the “Device.” The Device is currently located at a secured facility controlled by the Tulsa Police Department.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

### **Probable Cause**

7. On July 9, 2024, at approximately 3:00 p.m., officers with the Tulsa Police Department (“TPD”) responded to a “shots heard” call at 7473 E. 30th Place, which address is within the City of Tulsa. The caller reported that a white male in his 30’s, bearded and wearing a white shirt, was heard saying he was going to kill a female outside of the house at 7479 E. 30th Place. The caller also stated that he saw a white Dodge Charger leave the residence and drive east.

8. Officers responded to the area east of the home and tried to locate the car. When that effort failed, they went to the home. Parked outside of the home, officers observed the white Dodge Charger with the driver’s-side door open. The car appeared to be unoccupied. The car had an Oklahoma Cherokee license plate.<sup>1</sup> The

---

<sup>1</sup> The car belonged to the victim, who is Cherokee. The undersigned subsequently confirmed that Bryce Pyle is an enrolled member of the Muscogee (Creek) Nation through a certified Enrollment Verification.

two officers approached the house and car. While approaching, a white male with a beard and a gray tank top exited the front door of 7479 E. 30th Place and walked towards the front yard. Officers saw a tan pistol sticking out of his left pants pocket. Officers commanded the male to get on the ground. In response, the suspect threw the gun onto the yard and complied with officers' commands. The man, who identified himself as Bryce Pyle, was then taken into custody without incident.

9. Officers visually cleared the car to ensure that nobody else was in it. While doing so, officers observed two more firearms sitting in the front driver's-side seat in plain view: a black Glock pistol and a Draco pistol.<sup>2</sup> Officers also recovered the tan pistol that Pyle threw out of his pocket and onto the ground. That pistol was a FN Five-Seven MK3 semiautomatic firearm.

10. Officers then spoke with the victim, who had stepped out onto the front porch with her young daughter. The victim, J.M., stated that she was at home watching a movie with her boyfriend (not Pyle). Her daughter's father (Pyle) arrived unexpectedly. Pyle was not at any point in time invited into the home. J.M. stated that Pyle became enraged when he saw that her boyfriend was there. Pyle came to the front door and kicked the door open, breaking the door latch and causing damage to the doorframe. J.M. said that Pyle pointed his Draco at her and her boyfriend. J.M. said that she told Pyle to leave and threatened to call the police if he did not. Pyle returned to his vehicle and while driving away fired his gun from the driver's side

---

<sup>2</sup> A Draco is a semiautomatic pistol version of an AK-47, which is chambered in a 7.62 caliber and loaded with a 30-round magazine.

door, in J.M.'s direction, at least once.<sup>3</sup> J.M. said that Pyle then drove away eastward in the white Dodge Charger. At this point, their young daughter was still in the car with Pyle.

11. J.M. said that a short time later, after her boyfriend had left the home, Pyle returned to the residence. J.M. stated that Pyle entered the residence, intentionally broke J.M.'s television, and proceeded to J.M.'s bedroom, where he retrieved a tan pistol that belonged to him. Officers arrived a short time later while Pyle was exiting the front door with the tan pistol.

12. After speaking with J.M., officers started canvassing the area for spent casings. Officers located a spent 9mm Luger brass casing next to the curb in front of the house. The casing was close to where the Dodge Charger had been parked. Upon inspection, officers discovered that it was an FC brand casing and observed black powder residue caked on it. The casing was recovered and turned into evidence.

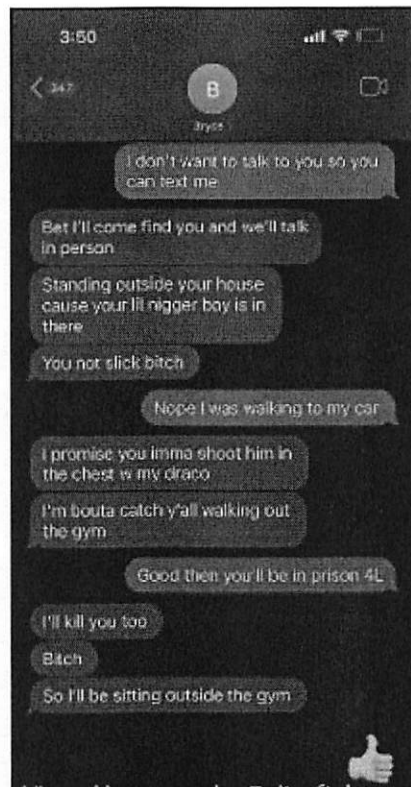
13. Officers then conducted a search of the vehicle and recovered the aforementioned Draco and Glock pistols. The Glock was chambered and magazine loaded with 9mm Luger FC brand brass ammunition. The Draco was magazine loaded with 7.62 brass ammunition. Officers also recovered a gray carbon fiber holster that fit a Glock. Officers also found Pyle's Oklahoma driver's license and an Apple iPhone 12 (the "Device"). All items were collected and turned into evidence.

---

<sup>3</sup> One shell casing was recovered, but no bullets.



14. Critically, while on scene, officers learned from J.M. that Pyle had been sending threatening text messages to her frequently. For example, the previous night, Pyle sent J.M. a text message referring to her boyfriend as a “lil’ n\*\*\*\*\* boy,” and “promis[ing]” to “shoot him in the chest with [his] draco.” Pyle continued: “I’ll kill you too . . . Bitch.” The picture below shows this portion of the text thread:



15. Officers canvassed nearby houses and noticed that the house directly across the street had a doorbell camera that possibly recorded the incident. Officers were later able to retrieve the video footage of this incident from the doorbell camera. The video footage corroborated J.M.’s recollection of the events. Among other things, the footage captured Pyle discharging his firearm, and showed J.M.’s reaction to the same.



16. Officers later contacted V.V., a next-door neighbor. V.V. said she saw some of the incident, and completed a witness statement stating as follows:

On July 9th around 2:30 pm I heard shouting outside my window. I don't remember if the voice was male or female. I looked outside my window and saw a man standing at the open right side of his car. It was a white mustang. He was looking at someone out of my view and said "I'm going to fucking kill you." He had his hands down facing the interior of the car. I heard him cock a pistol. I did not see the gun. I ran out of my room to tell my mom and heard two distinct gunshots. We then called the police. He was white, light brown or blonde hair, short on the side, slightly longer and curly on top. White tank top.

17. The Device is currently in the lawful possession of the Tulsa Police Department (TPD). It came into TPD's possession in the following way: the cell phone was seized as part of a search incident to arrest.

18. The Device is currently in storage at a secured facility controlled by the Tulsa Police Department. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Tulsa Police Department.

### **Technical Terms**

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data

communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This

storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using

specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be

used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. **Pager:** A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the

structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In addition, this cell phone will likely contain call logs and text messages, which, unless deleted, will contain calls and messages with J.M. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **Electronic Storage and Forensic Analysis**

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. Your affiant knows that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. Your affiant knows that in many cases, cellular telephones maintain photographs of illegal activities, including 18 U.S.C. §§ 1151, 1153, 21 O.S. §§ 1431, and 1436 – First Degree Burglary; 18 U.S.C. §§ 1151, 1153, and 113(a)(3) – Assault with Intent to do Bodily Harm in Indian Country; and 18 U.S.C. §

924(c)(1)(A)(iii) – Discharging a Firearm During and in Relation to a Crime of Violence. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. Your affiant also knows that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, your affiant knows that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

23. Your affiant knows that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like “Whatsapp” and “GroupMe.” Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include First Degree Burglary, Assault with Intent to do Bodily



Harm in Indian Country, and Discharging a Firearm During and in Relation to a Crime of Violence.

24. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

28. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

### **Conclusion**

29. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

30. Affiant requests to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

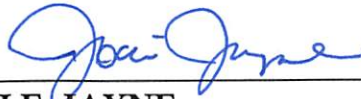
Respectfully submitted,



---

Special Agent Audra Rees  
Federal Bureau of Investigation

Subscribed and sworn to by phone on July 31, 2024.



---

**JODI F. JAYNE**  
**UNITED STATES MAGISTRATE JUDGE**

**ATTACHMENT A**

**Property to be Searched**

The property to be searched is an iPhone 12 taken off the person of Bryce Pyle incident to his arrest (the “Device”). The Device is currently located at a secured facility controlled by the Tulsa Police Department.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

## **ATTACHMENT B**

### **Particular Things to be Seized**

All records on the Device described in Attachment A that relate to violations of First Degree Burglary; 18 U.S.C. §§ 1151, 1153, and 113(a)(3) – Assault with Intent to do Bodily Harm in Indian Country; and 18 U.S.C. § 924(c)(1)(A)(iii) – Discharging a Firearm During and in Relation to a Crime of Violence involving Bryce Pyle, including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and

cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) listed above;
5. Threatening communications related to the criminal offense(s) listed above;
6. All bank records, checks, credit card bills, account information, and other financial records.
7. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
8. Records and information related to the geolocation of the Device and travel in furtherance of the criminal offenses listed above for the time period between June 8, 2024, and June 10, 2024; and
9. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been



created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.